UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,584	07/06/2001	Takehiko Nakano	SONYJP 3.0-187	4124

7590 10/12/2006

LERNER, DAVID, LITTENBERG, KRUMHOLZ & MENTLIK, LLP
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090-1497

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/900,584	**Applicant(s)** NAKANO, TAKEHIKO	
	Examiner David G. Cervetti	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 July 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6 and 8-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 8-15* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 July 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed July 17, 2006, have been fully considered.

2. Claims 1-6 and 8-15 are pending and have been examined. Claim 7 has been cancelled.

Response to Amendment

3. Applicant's arguments with respect to the prior art have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 2, 4-6, 8, and 10-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Misra et al. (US Patent 6,189,146, hereinafter Misra).

Regarding claim 1, Misra teaches an information processing apparatus for carrying out secure transmission of content to another apparatus over a network (fig 3), said information processing apparatus comprising:

- an encryption unit operable to encrypt the content (column 10, lines 2-37);
- an authentication unit operable to receive authentication information from the another apparatus when the another apparatus requests permission to

receive the encrypted content, and to determine whether the authentication information is valid (column 10, lines 38-67, fig 3, ref. 124);

- a first obtaining unit operable to obtain identification information of the another apparatus from the authentication information when the authentication information is valid and to determine whether the identification information of the another apparatus is already stored in a storage unit (column 10, lines 38-67, fig 3, ref. 124);
- a transmitting unit operable to transmit a decryption key to the another apparatus when the authentication information is valid and a count of a total number of apparatuses having permission to receive the encrypted content is less than a maximum value, the decryption key being needed to decrypt the encrypted content (column 10, lines 38-67, fig 3, ref. 126); and
- a first counting unit operable to increment by one the count of the total number of apparatuses having permission to receive the encrypted content when the identification information of the another apparatus is not already stored in said storage unit and the count of the total number of apparatuses having permission to receive the encrypted content is less than the maximum value (column 9, lines 1-36, table 3);
- said storage unit being operable to store the identification information of the apparatus when the identification information of the apparatus is not already stored in said storage unit (column 9, lines 37-67, table 4).

Regarding claims 4 and 5, Misra teaches a method for carrying out secure transmission of content from an information processing apparatus to another apparatus over a network (fig 3), said method comprising:

- encrypting the content (column 10, lines 2-37);
- receiving authentication information from the another apparatus when the another apparatus requests permission to receive the encrypted content (column 10, lines 38-67, fig 3, ref. 124);
- determining whether the authentication information is valid; obtaining identification information of the another apparatus from the authentication information when the authentication information is valid (column 10, lines 38-67, fig 3, ref. 124);
- determining whether the identification information of the another apparatus is already stored; transmitting a decryption key to the another apparatus when the authentication information is valid and a count of a total number of apparatuses having permission to receive the encrypted content is less than a maximum value, the decryption key being needed to decrypt the encrypted content (column 10, lines 38-67, fig 3, ref. 126);
- incrementing by one the count of the total number of apparatuses having permission to receive the encrypted content when the identification information of the another apparatus is not already stored and the count of the total number of apparatuses having permission to receive the encrypted

content is less than the maximum value (column 9, lines 1-36, table 3); and

- storing the identification information of the apparatus when the identification information of the apparatus is not already stored (column 9, lines 37-67, table 4).

Regarding claim 6, Misra teaches an information processing apparatus for carrying out secure receiving of content from a first apparatus over a first network connection and for carrying out secure transmission of the content to a second apparatus over a second network connection (fig 3), said information processing apparatus comprising:

- a first transmitting unit operable to transmit to the first apparatus a request for permission to receive the content (column 6, lines 45-67, column 7, lines 1-20);
- a first authentication unit operable to perform a first authentication procedure with the first apparatus (column 6, lines 45-67, column 7, lines 1-20);
- a receiver operable to receive a first decryption key from the first apparatus when the first authentication procedure is successful (column 6, lines 45-67, column 7, lines 1-20);
- a decryption unit operable to use the first decryption key to decrypt encrypted content received from the first apparatus (column 8, lines 35-67, column 7, lines 1-20);

- a reencryption unit operable to reencrypt the decrypted content (column 10, lines 2-37);
- a second authentication unit operable to receive authentication information from the second apparatus when a request for permission to receive the content is made from the second apparatus and to determine whether the authentication information is valid (column 10, lines 38-67, fig 3, ref. 124);
- a first obtaining unit operable to obtain identification information of the second apparatus from the authentication information when the authentication information is valid and to determine whether the identification information of the second apparatus is already stored in a storage unit (column 10, lines 38-67, fig 3, ref. 124);
- a second transmitting unit operable to transmit a second decryption key to the second apparatus when the authentication information is valid and a count of a total number of apparatuses having permission to receive the reencrypted content is less than a maximum value, the second decryption key being needed to decrypt the reencrypted content (column 10, lines 38-67, fig 3, ref. 126); and
- a first counting unit operable to increment by one the count of the number of apparatuses having permission to receive the reencrypted content when the identification information of the second apparatus is not already stored in said storage unit and the count of the total number of apparatuses having

permission to receive the reencrypted content is less than the maximum value (column 9, lines 1-36, table 3);

- said storage unit being operable to store the identification information of said second apparatus when the identification information of the second apparatus is not already stored in said storage unit (column 9, lines 37-67, table 4).

Regarding claims 10 and 11, Misra teaches a method for carrying out secure receiving of content from a first apparatus over a first network connection and for carrying out secure transmission of the content to a second apparatus over a second network connection (fig 3), said method comprising:

- transmitting to the first apparatus a request for permission to receive the content (column 6, lines 45-67, column 7, lines 1-20);
- performing a first authentication procedure with the first apparatus (column 6, lines 45-67, column 7, lines 1-20);
- receiving a first decryption key from the first apparatus when the first authentication procedure is successful (column 6, lines 45-67, column 7, lines 1-20);
- decrypting, using the first decryption key, encrypted content received from the first apparatus (column 8, lines 35-67, column 7, lines 1-20);
- reencrypting the decrypted content (column 10, lines 2-37);
- receiving authentication information from the second apparatus when a request for permission to receive the content is made from the second

apparatus; determining whether the authentication information is valid (column 10, lines 38-67, fig 3, ref. 124);

- obtaining identification information of the second apparatus from the authentication information when the authentication information is valid; determining whether the identification information of the second apparatus is already stored (column 10, lines 38-67, fig 3, ref. 124);
- transmitting a second decryption key to the second apparatus when the authentication information is valid and a count of a total number of apparatuses having permission to receive the reencrypted content is less than a maximum value, the second decryption key being needed to decrypt the reencrypted content (column 10, lines 38-67, fig 3, ref. 126);
- incrementing by one the count of the number of apparatuses having permission to receive the reencrypted content when the identification information of the second apparatus is not already stored in said storage unit and the count of the total number of apparatuses having permission to receive the reencrypted content is less than the maximum value (column 9, lines 1-36, table 3);
- storing the identification information of the second apparatus when the identification information of the second apparatus is not already stored (column 9, lines 37-67, table 4).

Regarding claim 2, Misra teaches wherein the another apparatus is operable to transmit the encrypted content to a plurality of further apparatuses over the network (fig 6, intermediate server), and said information processing apparatus further comprises:

- a second obtaining unit operable to obtain a first value and a second value from the another apparatus when the authentication information is valid, the first value being a number of apparatuses in the plurality of further apparatuses that are newly requesting permission to receive the encrypted content, and the second value being a total number of apparatuses in the plurality of further apparatuses (column 4, lines 30-67); and
- a second counting unit operable to increment the count of the total number of apparatuses having permission to receive the encrypted content by the first value when (i) the sum of the first value and the count of the total number of apparatuses having permission to receive the encrypted content is at most equal to the maximum value and (ii) the identification information of the another apparatus is already stored in said storage unit (column 11, lines 35-67),
- said second counting unit being operable to increment the count of the total number of apparatuses having permission to receive the encrypted content to receive the encrypted content by the second value when (i) the sum of the second value and the count of the total number of apparatuses having permission to receive the encrypted content is at most

equal to the maximum value and (ii) the identification information of the another apparatus is not already stored in said storage unit (column 11, lines 35-67).

Regarding claim 8, Misra teaches a third transmitting unit operable to transmit, to the first apparatus, the count of the number of apparatuses having permission to receive the content (abstract).

Regarding claim 12, Misra teaches wherein the authentication information includes first authentication information and second authentication information, and said authentication unit includes:

- a first authentication subunit operable to receive the first authentication information from the another apparatus when the another apparatus requests permission to receive the encrypted content, and to determine whether the first authentication information is valid (column 10, lines 38-67, fig 3); and
- a second authentication subunit operable to transmit a request for the second authentication information to the another apparatus when the first authentication information is valid, to receive the second authentication information from the another apparatus, and to determine whether the second authentication information is valid (column 10, lines 38-67);
- said transmitting unit being operable to transmit the decryption key to the apparatus when the second authentication information is valid

and the count of the total number of apparatuses having permission to receive the encrypted content is less than the maximum value (column 10, lines 38-67).

Regarding claim 13, Misra teaches wherein the authentication information includes first authentication information and second authentication information, and said second authentication unit includes:

- a first authentication subunit operable to receive the first authentication information from the second apparatus when the second apparatus requests permission to receive the content, and to determine whether the first authentication information is valid (column 10, lines 38-67, fig 3); and
- a second authentication subunit operable to transmit a request for the second authentication information to the second apparatus when the first authentication information is valid, to receive the second authentication information from the second apparatus, and to determine whether the second authentication information is valid (column 10, lines 38-67);
- said second transmitting unit being operable to transmit the second decryption key to the second apparatus when the second authentication information is valid and the count of the total number of apparatuses having permission to receive the re-encrypted content is less than the maximum value (column 10, lines 38-67).

Claim Rejections - 35 USC § 103

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 3 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Misra, and further in view of Yoshiura.

Regarding claims 3 and 9, Misra teaches using encryption, providing the different keys needed for decryption/encryption to the different parties, encrypting the content, and tracking/counting the devices having permission to receive a license (abstract, columns 4-5).

Misra does not expressly disclose updating the an information updating unit operable to delete the identification information stored in said storage unit and to reset the count of the total number of apparatuses to receive the encrypted/re-encrypted content when said (second) decryption key is changed.

However, Yoshiura teaches an information updating unit operable to delete the identification information stored in said storage unit and to reset the count of the total number of apparatuses to receive the encrypted/re-encrypted content when said (second) decryption key is changed (column 25, lines 1-67).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to delete information used for identification / authentication and reset a count value when a decryption key is changed. One of ordinary skill in the art would have been motivated to perform such a modification maintain security of the system even when keys are updated (Yoshiura, column 4).

8. Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Misra.

Regarding claims 14 and 15, Misra teaches wherein the another apparatus is operable to transmit the encrypted content to a plurality of further apparatuses over the network, and said method further comprises: obtaining a first value and a second value from the another apparatus when the authentication information is valid, the first value being a number of apparatuses in the plurality of further apparatuses that are newly requesting permission to receive the encrypted content, and the second value being a total number of apparatuses in the plurality of further apparatuses (column 4, lines 30-67).

Misra does not expressly disclose incrementing by a value x if a certain set of conditions is met or by another value if another set of conditions is met, but does disclose keeping track of how many and where the licenses are assigned (column 9, lines 1-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to replace the method Misra uses to keep track of the assigned/used licenses by any other method to achieve the same result. One of ordinary skill in the art would have been motivated to perform such a modification to keep track of assigned licenses.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

11. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

12. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DGC

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/09/06